Generació de volcans de 7-isogènies de corbes el·líptiques

Autor: Albert Ventura Aresté
Director: Josep M. Miret Biosca

Universitat de Lleida
Escola Politècnica Superior
Enginyeria Tècnica en Informàtica de Gestió

Treball de Fi de Carrera

Setembre de 2007

Índex

Índex de taules

Capítol 1

Introducció

La *Criptografia*[1] és l'art d'escriure amb clau secreta o d'una manera enigmàtica. No obstant és difícil determinar en quin moment l'home va començar a fer-ne ús d'ella; en qualsevol de les civilitzacions antigues, existeixen exemples de l'ús de la criptografia, es diu però que les primeres en usar-la van ser l'Egipci, la Mesopotàmia, la China i la Índia.

De l'Antic Egipte a la era digital, els missatges xifrats han jugat un paper important en la història, Armes de militars, de diplomàtics i espies, són la millor defensa de les comunicacions i de dades que viatgen per Internet. La necessitat de transmetre informació d'una manera segura és una prioritat i un desafiament tècnic d'alt nivell. Cada vegada més es requereixen noves tècniques i algorismes d'encriptació de dades per transmetre informació amb un alta seguretat a través d'internet o un altre medi de comunicació, o per protegir la informació.

La peça bàsica de la criptografia és el criptosistema o l'algorisme criptogràfic. Aquest és l'algoritme que converteix un text en clar en un text xifrat. Fins a mitjants de la dècada dels 70 només existia un algorisme criptogràfic, el simètric o de clau privada, on un dels seus principals inconvenients era i segueix sent, la distribució de claus. Al 1976, dos ingeniers de la Universitat de Standford, Whitfield Diffie i Martín Hellman [2] van començar una gran revolució, al dissenyar la criptografia de clau pública. La nova idea consistia en: un criptosistema on hi havia dos claus, una per xifrar i l'altre per desxifrar. El sistema es basa en que si dos persones volen intercanviar missatges, cadascuna crea la seva parella de claus i fa pública la clau de xifrat (clau pública). Aleshores la persona 1, fent ús de la clau de xifrat de la persona 2, compon i envia el seu missatge, la persona 2 al rebre'l podrà desencriptar-lo fent ús de la seva clau per desxifrar (clau privada). Les seves principals aplicacions són l'intercanvi de claus privades

[1] Criptografia prové de les paraules amb grec "kriptos"(ocult, secret) i "grafos"(escriptura)

i la firma digital.

En 1985, Neil Koblitz [6] i Victor Miller [8], de forma independent, van proposar el criptosistema de corba el·líptica de clau pública (ECC), on la seva seguretat computacional es basa en el problema del logaritme discret, i ofereix una gran ventatge sobre els criptosistemes ampliament usats i ja acceptats RSA, com per exemple operar amb claus de longitud de fins a 6 vegades més petites i oferint el mateix nivell de seguretat que RSA amb una longitud de clau de 1024 bits.

Aquest treball s'estudia els volcans de 7-isogènies de corbes el·líptiques. La importància d'aquests radica en el fet de que les corbes d'un mateix volcà comparteixen propietats criptogràficament interessants com per exemple el cardinal de la corba. El càlcul del cardinal d'una corba és un problema computacionalment molt costós, d'aquí ve la seva utilitat en criptografia. Mitjançant els volcans de 7-isogènies es pot trobar moltes corbes associades a una que tingui el cardinal criptogràficament adequat. Per tant, els algorismes que es donen en aquest treball per determinar el volcà associat a una corba el·líptica permet obtenir a partir d'una corba criptogràficament bona, una llista de corbes útils.

Aquest treball està organitzat de la següent manera: en el segon capítol es dona una introducció a les corbes el·líptiques que proporcionarà la base necessaria per compendre els capítols posteriors. En el capítol tercer s'expliquen primer les idees i conceptes necessaris, que després permetran veure l'estructura dels volcans de 7-isogènies i també s'estudia els algorismes que permeten la determinació de l'altura i el cràter del volcà. En l'últim capítol s'exposaran alguns dels resultats i de les proves fetes i les conclusions a les que s'han arribat.

Agraïments

Primer de tot vull agraïr al professor *Josep Maria Miret* per haver-me permès fer aquest projecte tan interessant, també pel seu esforç i dedicació en tot el projecte. Vull agraïr molt especialment l'ajuda de *Javier Valera* i la seva paciència a l'hora d'explicar-me aspectes difícils del projecte. Finalment dono gràcies als familiars, amics i companys que m'han escoltat quan no sabien el què escoltaven i m'han fet costat durant l'elaboració del projecte.

Capítol 2

Corbes El·líptiques

La major part de la informació s'ha extret de [5], de la tesis de Daniel Sardonil [11] i de la tesis de Ramiro Moreno [10].

2.1 Introducció a les corbes el·líptiques

Una corba el·líptica sobre un cos $\mathbb{K}$ ve definida per una equació de *Weierstrass*:

$$E/\mathbb{K} \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

on a_i són elements del cos $\mathbb{K}$, en el nostre cas $\mathbb{K} = \mathbb{F}_p$. On la corba no ha de tenir punts singulars, és a dir, que la funció

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,$$

tingui una de les seves derivades parcials $\frac{\partial f}{\partial x}$ o $\frac{\partial f}{\partial y}$ diferents de zero en tots els seus punts. O també, que és el mateix, el discriminant (Δ) de la corba ha de ser diferent de zero. El càlcul del discriminant de l'equació de la corba anterior, es pot realitzar seguint els següents passos:

$$\begin{aligned}
d_2 &= a_1^2 + 4a_2, \\
d_4 &= 2a_4 + a_1a_3, \\
d_6 &= a_3^2 + 4a_6, \\
d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\
\Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6.
\end{aligned}$$

Sigui E una corba el·líptica definida sobre $\mathbb{K}$, amb un cos de característica diferent de 2 o 3 ($p \neq 2, 3$). Llavors existeix un canvi de coordenades racional tal que E té una equació, anomenada *reduïda de Weierstrass* de la forma:

$$y^2 = x^3 + Ax + B,$$

on A,B $\in \mathbb{K}$ i el discriminant $\Delta = 4A^3 + 27B^2 \not\equiv 0$. LLavors, podem definir el conjunt de punts d'una corba el·líptica $E_{A,B}/\mathbb{K}$ com:

$$E_{A,B}(\mathbb{K}) = \{(x, y) \in \mathbb{K} \times \mathbb{K} \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}_{E_{A,B}}\}$$

on $\mathcal{O}_{E_{A,B}}$ és l'anomenat punt de l'infinit de la corba que permet dotar a aquest conjunt d'estructura de grup abelià.

2.2 Corbes el·líptiques sobre cossos $\mathbb{F}_p$

Una corba el·líptica sobre un cos finit $\mathbb{F}_p$, on p és un primer, ve definida per una equació de la forma:

$$y^2 = x^3 + Ax + B \pmod{p},$$

on A,B són elements de $\mathbb{F}_p$ i $4A^3 + 27B^2 \neq 0 \pmod{p}$. El conjunt de punts de la corba són els punts (x, y) tals que x i $y \in \mathbb{F}_p$ i que satisfan l'equació de la corba. Totes les propietats de les corbes el·líptiques sobre cossos, també són aplicables a les corbes el·líptiques sobre cossos $\mathbb{F}_p$, però aquests tenen una sèrie de característiques pròpies.

El cardinal d'una corba el·líptica E sobre $\mathbb{F}_p$, que denotem per $\#E(\mathbb{F}_p)$, és el nombre de punts amb coordenades a $\mathbb{F}_p$ que conté la corba, més el punt de l'infinit $\mathcal{O}_E$.

El teorema de Hasse acota el cardinal d'una corba el·líptica sobre un cos finit.

Teorema 1(*Hasse) Sigui E una corba el·líptica definida sobre un cos finit* $(\mathbb{F}_p)$*, i sigui* $m = \#E(\mathbb{F}_p)$*, llavors:*

$$p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p}.$$

Cal remarcar que el càlcul del cardinal d'una corba el·líptica és un problema computacionalment difícil. Tot i que hi ha algorismes polinòmics que el resolen, a la pràctica resulten ineficients.

Teorema 2 (*Waterhouse) Si* $m \in [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$*, llavors existeix una corba el·líptica E sobre* $\mathbb{F}_p$ *tal que,*

$$\#E(\mathbb{F}_p) = m.$$

Si $P \in E(\mathbb{F}_p)$, l'ordre d'aquest punt, que denotarem per $\#P$, és l'enter positiu n més petit tal que

$$nP = P + P + P + ... + P = \mathcal{O}_E.$$

Tenint en compte el teorema de Lagrange relatiu a les propietats dels grups finits, se satisfà:

$$\#P|\#E(\mathbb{F}_p).$$

2.3 Polinomi de 7-divisió

Per tal de trobar els punts d'ordre n de la corba $E_{A,B}/\mathbb{F}_p$, es necessita l'ús dels polinomis de divisió.
Cal saber que el polinomi de 7-divisió (Ψ_7) serà un polinomi de grau :

$$\frac{(\ell^2-1)}{2} = 24$$

Donada una corba $E_{A,B}/\mathbb{F}_p$ d'equació $y^2 = x^3 + Ax + B$, es defineixen els polinomis divisors $\Psi_n(x, y)$ tal que $n \in \mathbb{Z}_{\geq 0}$ amb les expresions recursives següents:

$$\begin{array}{lcl}
\Psi_0(x,y) & = & 0 \\
\Psi_1(x,y) & = & 1 \\
\Psi_2(x,y) & = & 2y \\
\Psi_3(x,y) & = & 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\Psi_4(x,y) & = & 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\Psi_{2n}(x,y) & = & \frac{\Psi_n(x,y)}{2y}(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2), \text{ si } n \geq 2 \\
\Psi_{2n+1}(x,y) & = & \Psi_{n+2}\Psi_n^3 - \Psi_{n+1}^3\Psi_{n-1}, \text{ si } n \geq 2
\end{array}$$

A partir del polinomi de divisió $\Psi_n(x, y) \in \mathbb{F}_p[x, y]$, es pot obtenir el polinomi $f_n(x) \in \mathbb{F}_p[x]$ seguint els següents passos:

• Es realitza el canvi de variables y^2 per $x^3 + Ax + B$ en el polinomi $\Psi_n(x, y)$ obtenint un nou polinomi $\Psi_n(x)$ que quan n és parell queda multiplicat per y.

• Es defineix el polinomi $f_n(x)$ com:

$$f_n(x) = \begin{cases} \Psi_n(x) & \text{si } n \text{ és senar,} \\ \\ \frac{\Psi_n(x)y}{\Psi_n(x,y)} & \text{si } n \text{ és parell.} \end{cases}$$

Després de definir el polinomi Ψ_n, es pot trobar el polinomi de 7-divisió (Ψ_7) i per fer-ho s'utilitzarà l'expressió $\Psi_{2n+1}(x,y)$ amb $n=3$ quedant de la següent forma:

$$\Psi_7 = \Psi_{2\cdot 3+1} = \Psi_5\Psi_3^3 - \Psi_4^3\Psi_2$$

Mirant el resultat que ens dóna Ψ_7, es pot veure que es necessiten un altre cop les expressions, en aquest cas per calcular Ψ_5:

$$\Psi_5 = \Psi_{2\cdot 2+1} = \Psi_4\Psi_2^3 - \Psi_3^3\Psi_1$$

I substituïnt finalment, el Ψ_7 per les seves expressions, s'obtindrà el polinomi de 7-divisió per una corba el·líptica donada per una equació en forma reduïda de *Weierstrass*:

$\Psi_7(x) = 7x^{24} + 308Ax^{22} + 3944Bx^{21} - 2954A^2x^{20} - 112ABx^{19} + (-19852A^3 - 42896B^2)x^{18} - 92568A^2Bx^{17} + (-35231A^4 - 571872AB^2)x^{16} + (-31808A^3B - 829696B^3)x^{15} + (-82264A^5 - 615360A^2B^2)x^{14} + (-161840A^4B - 2132480AB^3)x^{13} + (-111916A^6 - 297472A^3B^2 - 928256B^4)x^{12} + (-608160A^5B - 2603776A^2B^3)x^{11} + (-42168A^7 - 1192800A^4B^2 - 3293696AB^4)x^{10} + (-425712A^6B - 3727360A^3B^3 - 1555456B^5)x^9 + (15673A^8 - 831936A^5B^2 - 7069440A^2B^4)x^8 + (-53824A^7B - 1314560A^4B^3 - 7127040AB^5)x^7 + (14756A^9 - 190400A^6B^2 - 2293760A^3B^4 - 2809856B^6)x^6 + (57288A^8B - 168448A^5B^3 - 3698688A^2B^5)x^5 + (1302A^{10} + 134400A^7B^2 + 394240A^4B^4 - 3039232AB^6)x^4 + (1680A^9B + 152320A^6B^3 + 831488A^3B^5 - 802816B^7)x^3 + (196A^{11} + 3696A^8B^2 + 96768A^5B^4 + 544768A^2B^6)x^2 + (392A^{10}B + 7168A^7B^3 + 64512A^4B^5 + 229376AB^7)x - A^{12} + 160A^9B^2 + 3328A^6B^4 + 24576A^3B^6 + 65536B^8.$

2.4 Corbes el·líptiques amb punts d'ordre 7

Considerem una corba el·líptica en forma reduïda de Weierstrass

$$E : y^2 = x^3 + Ax + B, \text{ amb } A, B \in \mathbb{F}_p,$$

amb punts d'ordre 7, és a dir, amb punts $P \in E(\mathbb{F}_p)$ tals que $7P = P + P + P + P + P + P + P = \mathcal{O}_E$.

Anomenem subgrup de 7-torsió de $E(\mathbb{F}_p)$, i el representem per $E[7](\mathbb{F}_p)$, al grup de punts d'ordre 7 que pertanyen a $E(\mathbb{F}_p)$ juntament amb el punt de l'infinit $\mathcal{O}_E$, és a dir,

$$E[7](\mathbb{F}_p) = \{P \in E(\mathbb{F}_p) \ \mid \ 7P = \mathcal{O}_E\}.$$

Aquestes corbes poden tenir 6 o 48 punts d'ordre 7. En el primer cas $E[7](\mathbb{F}_p) \simeq \mathbb{Z}_7$, mentre que el segon $E[7](\mathbb{F}_p) \simeq \mathbb{Z}_7 \times \mathbb{Z}_7$. Per trobar els punts d'ordre 7 es calculen les arrels del polinomi de 7-divisió (Ψ_7) de la corba. Les arrels d'aquest polinomi són les abscisses dels punts d'ordre 7 de $E(\mathbb{F}_p)$. Per saber quants punts d'ordre 7 té una corba el·líptica E sobre $\mathbb{F}_p$ dependrà de si $p \equiv 2, 3, 4, 5, 6 \pmod 7$ o $p \equiv 1 \pmod 7$, casos en que variarà la factorització del polinomi Ψ_7.

2.5 Corbes el·líptiques isomorfes

Teorema 3 (A. J. Menezes [7]) *Les corbes el·líptiques $E_1/\mathbb{F}_p : y^2 = x^3 + Ax + B$ i $E_2/\mathbb{F}_p : y^2 = x^3 + A'x + B'$ són isomorfes sobre $\mathbb{F}_p$ si i només si existeix $u \in \mathbb{F}_p^*$ tal que $u^4A' = A$ i $u^6B' = B$. Si $E_1 \cong E_2$ sobre $\mathbb{F}_p$, aleshores l'isomorfisme és donat per:*

$$\phi : E_1 \to E_2,$$
$$\phi : (x, y) \mapsto (u^{-2}x, u^{-3}y),$$

o el que és equivalent,

$$\psi : E_2 \to E_1,$$
$$\psi : (x, y) \mapsto (u^2x, u^3y).$$

Pel nostre cas, si $E \cong E'$ en $\mathbb{F}_p$, tenim tres casos a considerar:

- si $A = 0$ i $B \neq 0$, aleshores $A' = 0$ i $B' \neq 0$ ($u^6 = \frac{B}{B'}$);
- si $A \neq 0$ i $B = 0$, aleshores $A' \neq 0$ i $B' = 0$ ($u^4 = \frac{A}{A'}$);
- si $A \neq 0$ i $B \neq 0$, aleshores $A' \neq 0$ i $B' \neq 0$ ($u^2 = \frac{A'B}{AB'}$).

Capítol 3

Generació de volcans de 7-isogènies de corbes el·líptiques

En aquest capítol s'explicarà com es genera un volcà de 7-isogènies a partir d'una corba el·líptica, exposant-se també totes les idees i conceptes necessaris per poder crear el cràter del volcà amb totes les seves isogènies. La major part de la informació s'ha extret de [5], [3] i dels treballs de fi de carrera de Jaume Alcazo [1] i Oriol Morelló i Sebastià Serramona [9].

3.1 Isogènies de grau 7 de corbes el·líptiques

Una isogènia entre dues corbes el·líptiques E i E' sobre $\mathbb{F}_p$ és una aplicació tal que:

$$\begin{array}{rccc} I: & E(\mathbb{F}_p) & \longrightarrow & E'(\mathbb{F}_p) \\ & (x,y) & \longrightarrow & (X(x,y),Y(x,y)) \\ & \mathcal{O}_E & \longrightarrow & \mathcal{O}_{E'} \end{array}$$

on X i Y són expressions racionals en les coordenades (x,y) i tal que l'element neutre de E satisfà $I(\mathcal{O}_E) = \mathcal{O}_{E'}$. Es diu llavors que E i E' són corbes isògenes.

Una de les propietats de les corbes isògenes és que tenen el mateix cardinal. A més, si I és una isogènia de E a E', llavors existeix una altra isogènia $\tilde{I}$, anomenada dual de I, de E' a E tal que

$$\tilde{I} \circ I = \ell_E \text{ i } I \circ \tilde{I} = \ell'_E,$$

on ℓ_E és l'operació de multiplicar per ℓ a E, és a dir:

$$\begin{array}{rcl} \ell_E : E & \longrightarrow & E \\ P & \longrightarrow & \ell \cdot P \end{array}$$

i a ℓ se l'anomena grau de la isogènia.

Aquest treball està centrat en l'estudi d'isogènies de grau 7. Pel que fa a les corbes el·líptiques s'ha treballat amb l'equació reduïda de *Weierstrass*, esmentada al capítol de corbes el·líptiques. Mitjançant el seu polinomi Ψ_7, podem trobar les seves arrels, que seran les abscisses dels punts racionals d'ordre 7 de la corba.

Utilitzant les *fórmules de Vélu*[12], tenint l'equació de la corba en forma *general de Weierstrass*,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

i un subgrup $E(\mathbb{F}_p)$, es podrà determinar la corba isògena a E de nucli aquest subgrup:

Sigui $F \subseteq E(\mathbb{F}_p)$ un subgrup cíclic finit. Aleshores es defineixen els subconjunts:

$$R \text{ tal que } \begin{cases} \text{F}-E[2](\mathbb{F}_p) = R \cup (-R) \\ R \cap (-R) = \emptyset \end{cases}$$
$$S = F \cap E[2](\mathbb{F}_p) - \{\mathcal{O}_E\}$$

Per cada punt $Q = (x_Q, y_Q)$ del conjunt $F - \{\mathcal{O}_E\}$ es defineixen les quantitats de:

$$\begin{aligned} &t_Q = 6x_Q^2 + b_2x_Q + b_4 \qquad si \;\; Q \in S, \\ &t_Q = 6x_Q^2 + b_2x_Q + b_4 \qquad si \;\; Q \notin S, \\ &u_Q = 4x_Q^3 + b_2x_Q^2 + 2b_4x_Q + b_6, \\ &t = \sum_{Q \in R \cup S} t_Q, \\ &w = \sum_{Q \in R \cup S} (u_Q + xt_Q), \end{aligned}$$

on

$$\begin{aligned} &b_2 = a_1^2 + 4a_2, \\ &b_4 = a_1a_3 + 2a_4, \\ &b_6 = a_3^2 + 4a_6. \end{aligned}$$

Finalment la corba isògena E' té per equació:

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'.$$

sabent que

$$\begin{aligned} a'_1 &= a_1, \\ a'_2 &= a_2, \\ a'_3 &= a_3, \\ a'_4 &= a_4 - 5t, \\ a'_6 &= a_6 - b_2 t - 7w. \end{aligned}$$

La isogènia així definida té grau $\#F$.

Per al nostre cas:

- $F = \{P, 2P, 3P, 4P, 5P, 6P, \mathcal{O}\}$, on P és un punt d'ordre 7 de $E(\mathbb{F}_p)$. Llavors:

$$R \text{ tal que } \begin{cases} \{P, 2P, 3P, 4P, 5P, 6P, \mathcal{O}_E\} - \{\mathcal{O}_E\} = R \cup (-R) \\ R \cap (-R) = \emptyset \end{cases}$$
$$S = F \cap E[2](\mathbb{F}_p) - \{\mathcal{O}_E\}$$

- $S = \emptyset$,
- $R = \{P, 2P, 3P\}$.

També s'explicarà mitjançant un algorisme, com es troben tots els subgrups cíclics F d'ordre 7 d'una corba el·líptica definits sobre $\mathbb{F}_p$ generat per punts racionals d'ordre 7. Cal dir, que podrem tenir 0 o 1 o 8 isogènies , ja que podem tenir 0 o 1 o 8 subgrups cíclics (F).

Algorisme *Cerca subgrups cíclic (F)*

Entrada: El polinomi de 7-divisió Ψ_7.
Sortida: Els grups cíclics F.

---

funció cercar F (Ψ_7)

mentres $\exists$ **arrel de** Ψ_7 **fer**
r:=arrel (Ψ_7);
Ψ_7**:=**$\frac{\Psi_7}{x-r}$; */*S'elimina l'arrel r de* Ψ_7 **/*
si r $\in$ **a un punt racional llavors**
P:=(r,s); */*Es construeix el punt P a partir de r, que serà l'abscissa de P*/*
Ψ_7**:=**$\frac{\Psi_7}{x-abscissa(2P)}$; */*S'elimina l'abscissa del 2P de* Ψ_7 **/*
Ψ_7**:=**$\frac{\Psi_7}{x-abscissa(3P)}$; */*S'elimina l'abscissa del 3P de* Ψ_7 **/*

$F :=< P >$;
fsi
$F := \{P, 2P, 3P, -P, -2P, -3P, \mathcal{O}_E\} = \{P, 2P, 3P, 4P, 5P, 6P, \mathcal{O}_E\}$
fmentres
retorna F; */*Retornarà ∅ o una F o vuit F*/*

ffunció

Cal dir però, que per tal de començar amb corbes de punts racionals d'odre 7, s'ha treballat inicialment amb una *equació de la corba* del següent tipus:

$$E : y^2 + (1 + c - c^2)xy + c^2(1 - c)y = x^3 + c^2(1 - c)x^2,$$

on $c \neq 0, 1$ ja que el discriminant $\Delta = c^7(c - 1)^7(c^3 - 8c^2 + 5c + 1)$ dóna 0 quan c=0,1.

Aquesta equació ens assegura que la corba que s'agafa inicialment és bona, és a dir, que té punts d'ordre 7.

Donada aquesta corba E, s'utilitza també les *fórmules de Vélu* per trobar una corba isògena E'.

Per trobar les 7-isogènies caldrà determinar els punts d'ordre 7 de la corba, cosa que dependrà de si $p \equiv 2, 3, 4, 5, 6 \pmod 7$ o $p \equiv 1 \pmod 7$, casos que es detallaran en les següents subseccions.

3.1.1 Calculant les isogènies a $p \equiv 2, 3, 4, 5, 6 \pmod 7$

Quan $p \equiv 2, 3, 4, 5, 6 \pmod 7$ la corba $E : y^2 = x^3 + Ax + B$, només tindrà 6 punts d'ordre 7 en $\mathbb{F}_p$ i per tant un únic subgrup cíclic format per $\{P, 2P, 3P, 4P, 5P, 6P\} \subseteq E(\mathbb{F}_p)$, el qual només generarà una corba isògena a E. Amb el que s'ha explicat a l'apartat 3.1, tenint aquest subgrup i utilitzant les *fórmules de Vélu* es podrà generà la única corba isògena a E.

En algun cas, la corba E té altres punts no racionals d'ordre 7 i per tant no s'utilitzaran en aquest treball per calcular isògenes.

3.1.2 Calculant les isogènies a $p \equiv 1 \pmod 7$

Quan $p \equiv 1 \pmod 7$, la corba $E : y^2 = x^3 + Ax + B$, tal com s'ha dit abans, pot tenir 6 punts d'ordre 7, els quals permetran buscar una única isogènia, o bé 48 punts d'ordre 7. En aquest segon cas, s'hauran d'agrupar,

de sis en sis, forman 8 subgrups de punts d'ordre 7, cadascun dels quals determinarà una isogènia, en total hi haura 8 corbes isògenes a E.

3.2 Volcans de 7-isogènies de corbes el·líptiques

Recorrent de forma sistemàtica les 7-isogènies d'una corba inicial d'equació

$$E : y^2 = x^3 + Ax + B$$

es genera una estructura matemàtica coneguda com volcà de 7-isogènies associat a la corba E, i que es denotarà per V_E.

El volcà de 7-isogènies associat a una corba el·líptica és un graf orientat o digraf V, que consta d'un cicle de nodes anomenat cràter de cadascun dels quals en penjen 6 nodes (que suposarem en un nivell inferior). De cadascun d'aquests nodes penjen arbres 7-aris complets amb totes les fulles al mateix nivell. El conjunt de nodes del digraf està format per classes d'isomorfia de corbes el·líptiques i el conjunt d'arestes representa les 7-isogènies entre les corbes de cada node. Si dos nodes estan connectats per una aresta existeix una 7-isogènia I que transforma la corba E_1 d'un dels nodes, en una altra E_2 de l'altre node, llavors també existeix una altre aresta en l'altre sentit que representa la 7-isogènia dual $\hat{I}$.

Aquest digraf té la forma d'un volcà on els nodes estan separats en nivells. El nombre de nivells menys 1 és l'altura del volcà. El nivell superior o cràter del volcà pot estar format per:

- Un únic node.
- Dos nodes adjacents.
- Un cicle de longitud n, on $n > 2$.

Tots els nodes del volcà tenen 8 arestes dirigides cap a altres nodes, excepte els nodes que estan al nivell 0, el nivell de terra, que únicament tenen una aresta ascendent cap a un node del primer nivell.
Una de les principals propietats dels volcans és que estan formats per corbes el·líptiques isògenes entre sí, i per tant comparteixen el mateix cardinal.

3.3 Algorismes sobre volcans de 7-isogènies

En aquest apartat es presenteran els algorismes que ens permeten determinar l'altura i la longitud del cràter de volcans de 7-isogènies de corbes el·líptiques. Per calcular l'altura del volcà s'ha utilitzat un algorisme, que

per poder-lo explicar es diferenciaran dos casos $p \equiv 2, 3, 4, 5, 6 \pmod 7$ i $p \equiv 1 \pmod 7$, ja que la manera de recórrer el cràter serà diferent.

3.3.1 Cas $p \equiv 2, 3, 4, 5, 6 \pmod 7$

En aquest primer cas els volcans sempre seran d'altura 0 i per tant només estaran formats pel cràter. Com que de cada node només pot existir una isogènia de nucli un grup de punts racionals, s'ha d'agafar l'únic camí que hi ha fins a tornar a trobar-nos amb el node inicial, aleshores serà quan el cràter del volcà s'haurà tancat. Els passos que es segueixen en aquest cas són:

1. Obtenir inicialment una equació de la corba que tingui punts d'ordre 7, que l'anomenem *E*.

2. Un cop tenim *E*, es troba una corba isògena a ella, que l'anomenem *E'*, i comprovem que aquesta no sigui isomorfa a *E*, en aquest cas, ens voldrà dir que el cràter del volcà que estem estudiant, és un cràter amb una única corba.

3. Si la corba *E'* no és isomorfa a *E*, seguirem buscant una corba isògena a *E'*, que l'anomenem *E"*, i tornarem a comprovar si és isomorfa a *E* i si és així tancarem el cràter del volcà. Sinó és isomorfa tornarem a fer el mateix, trobar una isògena a *E"*, i així successivament fins a trobar una isògena que sigui isomorfa a la primera. Aleshores tancarem el cràter sense comptar aquesta última corba i ja tindrem el cràter creat i les corbes que la formen.

A continuació es mostra l'algorisme en pseudocodi, tot i que abans cal explicar les funcions que s'utilitzen en el pseudocodi:

-***boolea isomorfisme(corba el·líptica*** *E*, ***corba el·líptica*** *e)*: Retorna cert, si E i e són isomorfes i fals en cas contrari.

-***polinomi pol7divisio(corba el·líptica*** *E)*: Retorna el polinomi de 7 divisió de la corba el·líptica que li entrem.

-***vector troba_ arrels (polinomi*** *Poli)*: Retorna un vector amb totes les arrels del polinomi de divisió que li entrem.

-***boolea trobar_ isogenies (corba el·líptica*** E***, vector*** vec***, corba el·líptica*** $\&$ e***, vector de corbes el·líptiques*** $\&$ $vector\_corb$***)***: Retorna cert si troba una isògena a E i fals en cas contrari. Si troba una isogènia la guarda a e i si en troba més d'una (no és el cas) les guarda en $vector\_corb$.

Algorisme *Creació_ del _ cràter1*

Entrada: Un primer $p \equiv 2, 3, 4, 5, 6 \pmod 7$ i una corba amb punts d'ordre 7 definida sobre $\mathbb{F}_p$.
Sortida: La longitud del cràter c.

---

funció determinació_ crater2 (p,E**) retorna** c

```
c=1;
isogenia := trobar_ isogenia(E,vec,e,vec_ corb);
isomorfia := isomorfisme(E,e);
  mentre  isomorfia sigui fals  fer
    c:=c+1;
    pol := pol7divisio(e);
    vec := trobar_ arrels(pol);
    isogenies := trobar_ isogenies(e,vec,ell,vector_ corbes);
    e := ell;
    isomorfia := isomorfisme(E,e);
  fmentre
 retorna c;
```

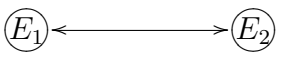
ffunció

- ***Exemples de volcans:***

Cal dir que una corba $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, serà representada com a $E = [(a_1), (a_2), (a_3), (a_4), (a_6)]$.

Exemple 1:

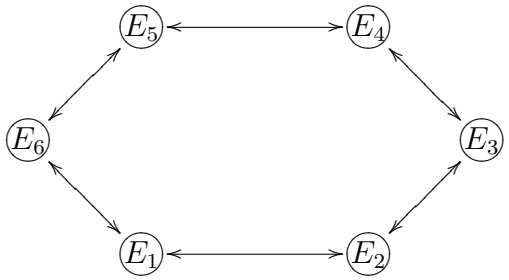
- p=37
- c=885
- E_1=[(26),(36),(36),(0),(0)], E_2=[(26),(36),(36),(16),(34)]



Volcà d'altura 0 amb 2 nodes (corbes) al cràter.

Exemple 2:

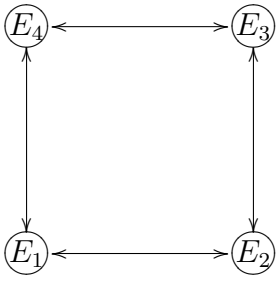
- p=419
- c=894
- E_1=[(273),(148),(148),(0),(0)]
- E_2=[(273),(148),(148),(209),(381)]
- E_3=[(273),(148),(148),(234),(227)]
- E_4=[(273),(148),(148),(306),(360)]
- E_5=[(273),(148),(148),(188),(244)]
- E_6=[(273),(148),(148),(156),(222)]



Volcà d'altura 0 amb 6 nodes (corbes) al cràter.

Exemple 3:

- p=601
- c=478
- E_1=[(375),(275),(275),(0),(0)]
- E_2=[(375),(275),(275),(431),(223)]
- E_3=[(375),(275),(275),(416),(120)]
- E_4=[(375),(275),(275),(359),(597)]



Volcà d'altura 0 amb 4 nodes (corbes) al cràter.

3.3.2 Cas $p \equiv 1 \pmod 7$

En aquest segon cas, ens podem trobar amb volcans d'altura 0 o volcans d'altura més gran que 0. Si el volcà és d'altura 0, se seguirà el mateix procediment que a l'apartat 3.3.1 i si el volcà és d'altura més gran que 0 s'haurà de buscar l'altura del volcà i un cop trobada, ja podrem trobar tots els nodes (corbes) que formen el cràter del volcà. Els passos que se segueixen en aquest cas són:

1. Obtenir inicialment una equació de la corba que tingui punts d'ordre 7, que l'anomenem E.

2. Un cop tenim E s'haurà de calcular el nivell de la corba en el volcà, per saber la seva ubicació en el volcà. Ens podem trobar amb dos casos:

-La corba E estigui a nivell 0 i el volcà tingui altura 0, voldrà dir que ja estem al cràter del volcà.

-La corba E estigui en un nivell ≥ 0 i el volcà sigui d'altura > 0. Per fer això ens valdrem d'una funció (que en el treball s'anomena Nivell), que ens dóna la informació del *nivell del volcà* en que està la corba, d'aquesta manera ens ajuda a escalar el volcà.

3. A partir d'aquesta corba, s'ha d'arribar al cràter i comencem buscant les seves corbes isògenes, que podran ser una (voldrà dir que la corba E està a nivell 0) o vuit (voldrà dir que E està a un nivell > 0):

-Si la corba isògena que hem trobat es troba en un nivell inferior, ignorem aquesta corba i en busquem una altra.

-Si la corba es troba en un nivell superior, busquem les corbes isògenes d'aquesta nova corba seguint el mateix criteri.

-Si la corba es troba en el mateix nivell, significa que ambdues pertanyen al cràter.

-Si totes les corbes isògenes estan en un nivell inferior, aleshores tindrem un volcà amb una sola corba al cràter (mirar exemple 3).

4. Un cop arribem al cràter per recórrer tots els seus nodes, no ens interessa baixar d'aquest nivell i el que farem serà buscar les isogènies que estiguin en aquest nivell, fins a trobar la isògena que sigui isomorfa a la primera corba. Aleshores tancarem el cràter sense comptar aquesta última corba i ja tindrem el cràter creat i les corbes que la formen.

A continuació es mostra l'algorisme en pseudocodi, tot i que abans cal explicar les funcions que s'utilitzen en el pseudocodi:

-***enter Nivell (corba el·líptica E)***: Aquesta funció és la que busca el nivell de la corba dins del volcà. Per tal de trobar el nivell on es troba la corba E, s'utilitza el següent mètode:

Primer busca les isògenes de E:

- Si només té una isògena $nivell(E) = 0$.

- Si té 8-isogènies, s'ha de calcular un camí descendent des de E fins a una corba el·líptica situada al *terra del volcà*. Aleshores, la longitud d'aquest camí és el nivell on es troba E. Aquest camí descendent, que tindrà longitud k, és una successió d'isogènies $E \to E_1 \to E_2 \to ... \to E_k$, on totes les corbes isògenes estaran en un nivell inferior que les seves anteriors, és a dir,

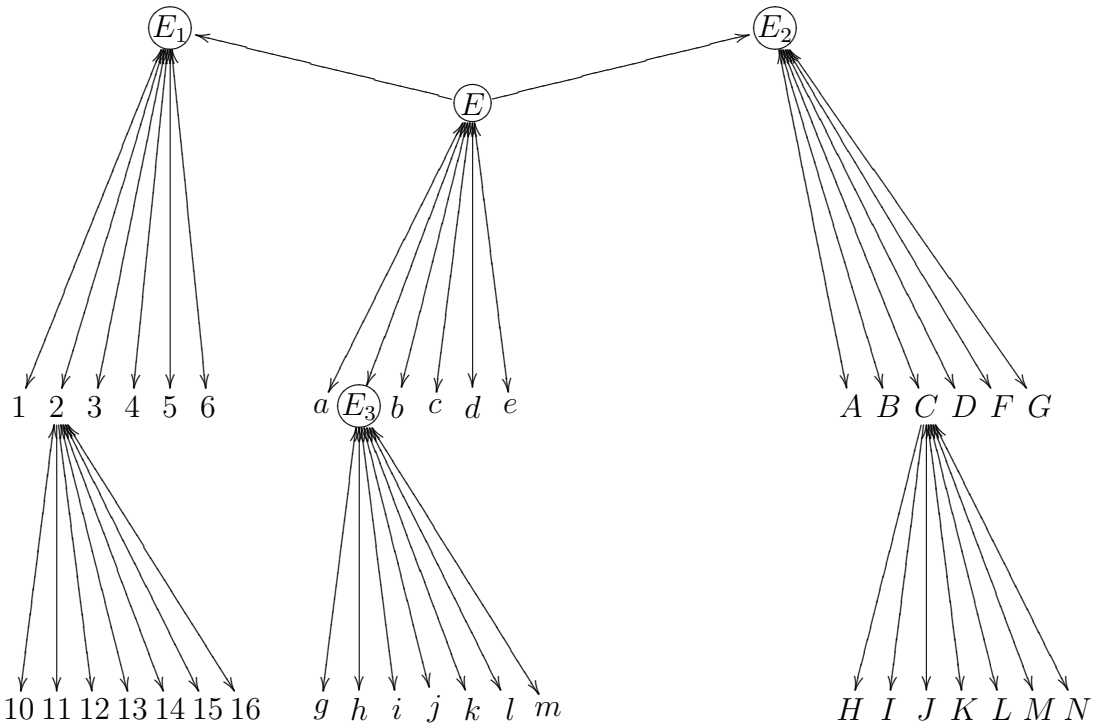
  $$nivell(E_i) = i \text{ i } nivell(E_{i+1}) = i - 1.$$

  Per trobar aquest camí s'han d'agafar 3 corbes isògenes de les vuit que té E. D'aquesta manera ens assegurem que un camí dels 3 serà un camí descendent fins al terra.

A continuació s'expliquen dos possibles casos que es poden trobar a la cerca del nivell d'una corba i que ens permetran veure amb més claredat el funcionament de la funció Nivell:

Cas 1: La corba E es troba al cràter d'un volcà d'altura>0.

• Les 3 corbes isògenes a E que agafem són E_1, E_2, E_3, que estaran al Camí1, Camí2, Camí3 respectivament. També s'ha de dir que els dos volcans representats arriben fins al terra del volcà.



Possibles camins:

Camí1:$E \longrightarrow E_1 \longrightarrow 2 \longrightarrow 10$.

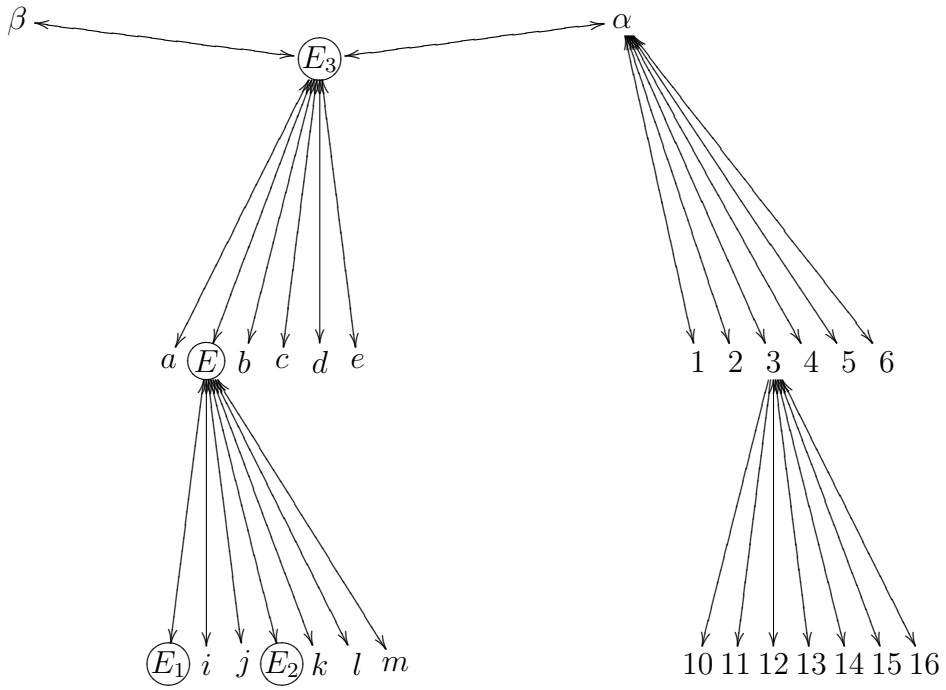
Camí2:$E \longrightarrow E_2 \longrightarrow C \longrightarrow J$.

Camí3:$E \longrightarrow E_3 \longrightarrow h$.

Es pot veure que el camí més curt és el *Camí3*, per tant $nivell(E)= 2$.

Cas 2: La corba E es troba al mig del volcà d'altura>0.

•Les 3 corbes isògenes a E que agafem són E_1, E_2, E_3, que estaran al Camí1, Camí2, Camí3 respectivament.



Possibles camins:

Camí1:$E \longrightarrow E_1$.

Camí2:$E \longrightarrow E_2$.

Camí3:$E \longrightarrow E_3 \longrightarrow \alpha \longrightarrow 3 \longrightarrow 12$.

Es pot veure que els camins més curts són *Camí1*, *Camí2* per tant $nivell(E)= 1$.

A continuació es mostra la funció nivell amb pseudocodi:

Algorisme *Trobar nivell(E)*

Entrada: Un primer $p \equiv 1 \pmod 7$ i una corba amb punts d'ordre 7 definida sobre $\mathbb{F}_p$.
Sortida: El nivell n de la corba E.

```
funció Nivell (p,E) retorna n

  isogenia = Trobar_ isogenia(E,vec,e,I)
  si Cardinal(I) != 8 llavors
    n := 0;
  sino
    i := 0;
    Q := [ ]; /*Són els passos de cada camí*/
    U := [ ]; /*Les corbes anteriors dels tres camins*/
    V := [ ]; /*Les corbes actuals dels tres camins*/
    W := [ ]; /*Vector de corbes isògenes de les corbes actuals (a cada
                posició hi ha un vector de corbes isògenes a una de les
                actuals)*/
      fer
        i +:= 1;
        Q[ i ] := 1;
        U[ i ] := E;
        V[ i ] := I[ i ];
        W[ i ] := Y( V[ i ] );
        a := Cardinal(W[ i ]) eq 1;
      mentres a sigui cert o i==3;
      mentres !a fer
        i := 0;
        fer
          i++;
          Q[ i ]++;
           si isomorfisme( U[ i ] , W[ i ][ 1 ] ) llavors
             U[ i ] := V[ i ];
             V[ i ] := W[ i ][ 2 ];
          sino
             U[ i ] := V[ i ];
             V[ i ] := W[ i ][ 1 ];
          end if;
          W[ i ] := Y( V[ i ] );
          a := Cardinal(W[ i ]) == 1;
         mentres a sigui cert o i==3;
      fmentre
      n := Q[ i ];
  fsi
  retorna n;

ffunció
```

-***vector de corbes fercami (corba el·líptica*** E***)***: Aquesta funció és la que recorre el volcà fins arribar al cràter i aleshores recorre el cràter i guarda les seves corbes a *vector de corbes*. Per tal d'arribar al cràter s'utilitza el mateix mètode que s'ha explicat al punt 3.

Algorisme *Creació_ del _ cràter2*

Entrada: El primer $p \equiv 1 \pmod 7$ i una corba amb punts d'ordre 7 definida sobre $\mathbb{F}_p$.
Sortida: L'altura h del volcà i les corbes que formen el cràter del volcà.

---

funció determinació_ crater2 (p**,**E**) retorna** h **i vector_corbes**

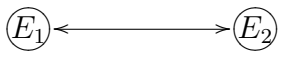
vector_ corbes:=fercami(E);
h:=Nivell(vec[0]);
retorna h,vector_corbes;

ffunció

- ***Exemples de volcans:***

Exemple 1:

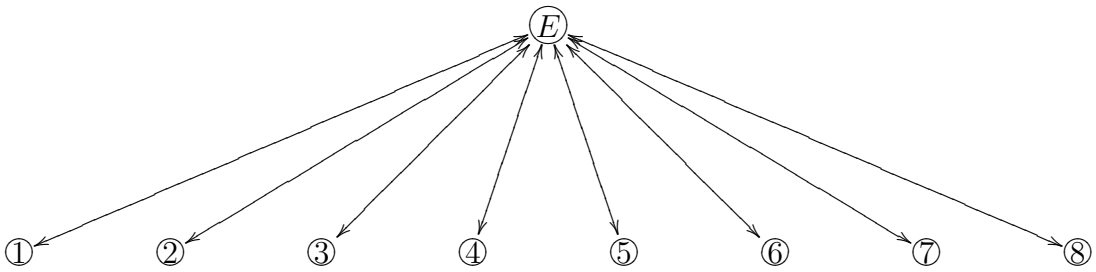
- p=13679
- c=688699
- E_1=[(8420),(11793),(11793),(0),(0)]
- E_2=[(8420),(11793),(11793),(5619),(10759)]



Volcà d'altura 0 amb dos nodes (corbes) al cràter.

Exemple 2:

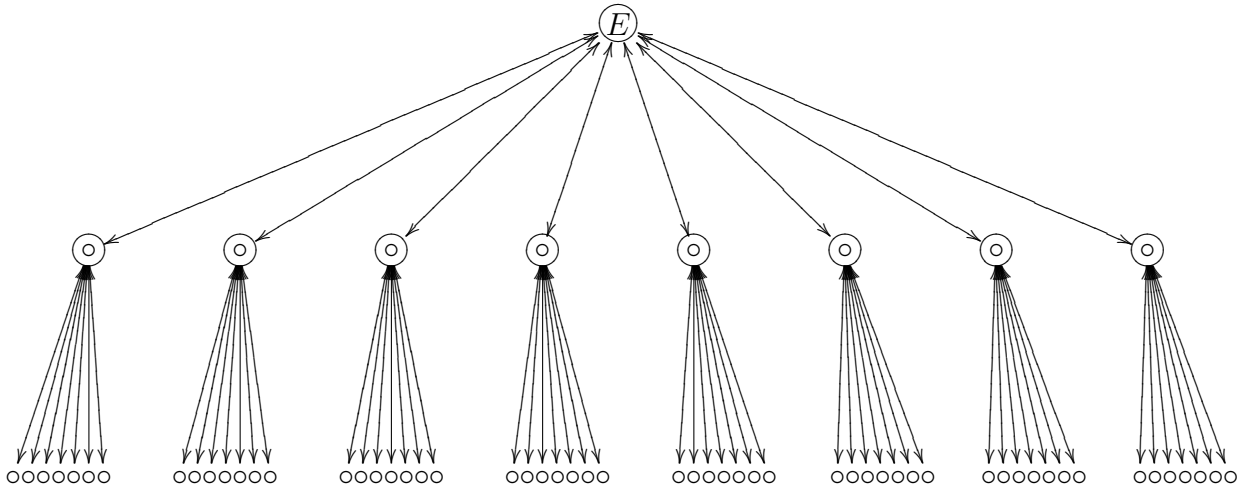
- p=167413
- c=675039
- E=[(115481),(151465),(151465),(0),(0)]



Volcà d'altura 1 amb un sol node (corba) al cràter.

Exemple 3:

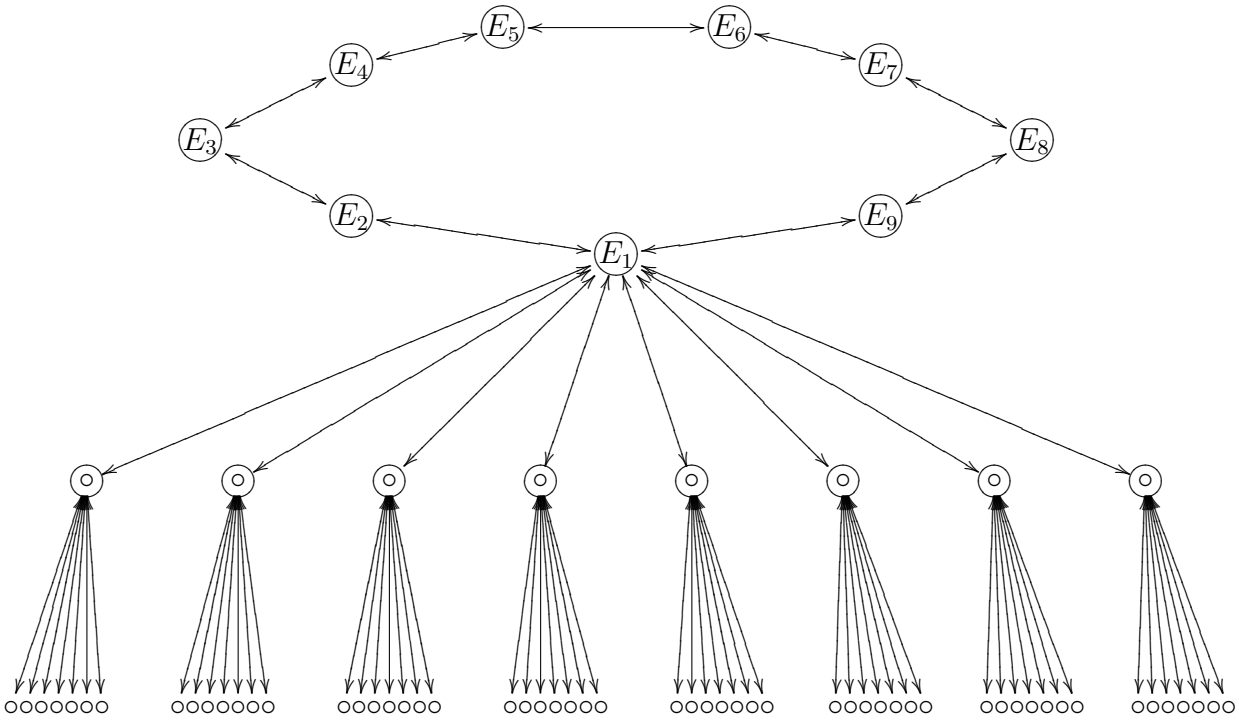
- p=6984139
- c=811791797
- E=[(5623684),(5448594),(5448594),(0),(0)]



Volcà d'altura 2 amb un sol node (corba) al cràter.

Exemple 4:

- p=204294679
- c=630246997
- E_1=[(187834686), (146460588), (146460588), (47492552), (39965218)]
- E_2=[(187834686), (146460588), (146460588), (181473460), (42805456)]
- E_3=[(187834686), (146460588), (146460588), (101344286), (162247460)]
- E_4=[(187834686), (146460588), (146460588), (3866678), (133292638)]
- E_5=[(187834686), (146460588), (146460588), (191274431), (77297033)]
- E_6=[(187834686), (146460588), (146460588), (127891770), (54089933)]
- E_7=[(187834686), (146460588), (146460588), (111329134), (144351293)]
- E_8=[(187834686), (146460588), (146460588), (26934494), (96812133)]
- E_9=[(187834686), (146460588), (146460588), (128617326), (158637069)]



Volcà d'altura 2 amb nou nodes (corbes) al cràter.

Capítol 4

Resultats i Conclusions

En aquest capítol es mostren exemples de resultats obtinguts utilitzant l'algorisme que s'ha implementat, el de la generació de volcans de 7-isogènies, comentan els valors de les taules mostrades. Més endavant ambé s'exposen les conclusions a les que he arribat i les futures línies de treball.

4.1 Resultats experimentals

Degut a la diferent estructura interna dels volcans sobre $\mathbb{F}_p$ quan $p \equiv 1 \pmod 7$ i quan $p \equiv 2, 3, 4, 5, 6 \pmod 7$ s'ha cregut oportú separar l'estudi experimental per aquests dos casos.

• **Volcans de 7-isogènies sobre $\mathbb{F}_p$ quan $p \equiv 1 \pmod 7$**

Tot seguit es mostra en les taules amb els resultats dels càlculs obtinguts quan $p \equiv 1 \pmod 7$. La notació utilitzada a la taula és la següent: la primera columna hi ha el primer p, la segona columna hi ha la variable c que genera la primera corba el·líptica, la tercera columna ens diu el número de corbes que formen el cràter del volcà, l'última columna ens mostra l'altura del volcà generat.

En la taula 4.1 es pot observar el recorregut en detall de tots els volcans definits sobre el cos $\mathbb{F}_{113}$. Amb aquesta taula i la 4.5, per tal de que a la taula no hi hagi volcans repetits, s'ha utilitzat el j-invariant de cada corba del cràter, que ens diu que si dos volcans tenen els mateixos j-invariants són iguals.

En la taula 4.2 es pot observar volcans amb altura>0.

En la taula 4.3 es pot observar volcans amb un cràter molt gran, són els més grans que he trobat amb altura>0.

$p = 113$		
c	#Corbes Cràter	altura
2	2	0
3	2	0
4	2	0
5	2	0
6	2	0
7	2	0
9	2	0
10	1	1
13	2	0
20	2	0
21	2	0
22	2	0
34	1	0
35	2	0
40	2	0
66	1	0

Taula 4.1: Recorregut de tots els volcans de 7-isogènies generats sobre $\mathbb{F}_{113}$.

- **Volcans de 7-isogènies sobre $\mathbb{F}_p$ quan** $p \equiv 2, 3, 4, 5, 6 \pmod 7$

Tot seguit es mostren les taules amb els resultats dels càlculs obtinguts quan $p \equiv 2, 3, 4, 5, 6 \pmod 7$. La notació és la mateixa utilitzada anteriorment però com que se sap que l'altura sempre serà 0, l'última columna no cal posar-la.

En la taula 4.4 es pot observar volcans amb un cràter molt gran, són els més grans que he trobat amb altura=0.

En la taula 4.5 es pot observar el recorregut en detall de tots els volcans definits sobre el cos $\mathbb{F}_{101}$. Es pot veure que als volcans amb altura=0 es troben cràters elevats amb més facilitat.

p	c	#Corbes Cràter	altura
164249	150538	2	1
29303	631943	13	1
204294679	630246997	9	2
6984139	811791797	1	2
93787	923154	1	3

Taula 4.2: Diferents volcans de 7-isogènies amb altura més gran que 0.

p	c	#Corbes Cràter	altura
51355753	35338362	152	1
9828617	780011514	214	1
606614303	323664821	306	1
2194803857	814792831	352	1
1052593823	919091187	902	1
2017138537	430924811	918	1
1037824621	411	1492	1

Taula 4.3: Diferents volcans de 7-isogènies amb altura>0 i el cràter elevat.

p	c	#Corbes Cràter
52912943	666566060	677
194554567	145835507	1622
422867407	632633819	2392
1365978623	788903290	2912
1739466811	105574593	5208
1824200531	832752617	17064
1477227671	405354742	23394

Taula 4.4: Diferents volcans de 7-isogènies amb altura=0 i el cràter elevat.

$p = 101$	
c	#Corbes Cràter
2	4
3	4
5	8
8	6
12	2
13	3
16	3
19	2
46	1

Taula 4.5: Recorregut de tots els volcans de 7-isogènies generats per $\mathbb{F}_{101}$.

4.2 Conclusions i futures línies de treball

Una vegada s'han vist els resultats, és pot veure que s'ha generat una llibreria que conté la implementació de tots els coneixements i algorismes explicats durant el treball així com d'alguns que s'han necessitat, que permeten generar i treballar amb volcans de 7-Isogènies de corbes el·líptiques definits sobre $\mathbb{F}_p$ on p és un primer. Aquests algorismes ens permeten conèixer tota la informació d'un volcà de 7-isogènies, com la seva altura i les corbes que formen el seu cràter.

Pel que fa a les futures línies de treball es podrien plantejar les següents millores sobre els algorismes de volcans:

1 . En la linia d'ampliar la llibreria de volcans es podria, i de fet s'hauria d'incorporar els algorismes que permetin reconèixer volcans degenerats. Aquests constitueixen una raresa en el món dels volcans, en que l'estructura del seu cràter és diferent de la que s'ha vist fins ara. Són volcans amb cràters d'un o dos nodes, on es poden observar, per exemple, isogenies reflexives (l'origen i el desti són la mateixa corva),...

2 . El que es podria fer i que de fet s'està fent, és realitzar un sòl algorisme que ens permeti generar volcans de 2-isogènies, 3-isogènies, 5-isogènies, 7-isogènies,..., és a dir, un algorisme general que li entris una corba el·líptica, el grau de les isogènies (l) i amb una p qualsevol ens calculi el volcà generat per aquests tres paràmetres *(Volcà de l-isògenies sobre $\mathbb{F}_p$)*.

Bibliografia

[1] J. Alcazo. *Creació de volcans de 3-isogènies de corbes el·líptiques*. Treball de Fi de Carrera, Universitat de Lleida, Juny 2005.

[2] W. Diffie and M. E. Hellman. *New directions in cryptography*. IEEE Trans. Inform. Theory IT-22, pages 644-654, 1976.

[3] M. Fouquet and F. Morain. *Isogeny Volcanoes and the SEA Algorithm. ANTVS-V, LINCS 2369*. 2002.

[4] LiDIA Group. *LiDIA, a library for computational number theory. Reference Manual*. http://www.informatik.tudarmastadt.de/TI/LiDIA, 2.1 edition, May 2001.

[5] C. Ivorra. *Curvas Elípticas*. http://www.uv.es/ivorra/Libros, Universitat de València, 2006.

[6] N. Koblitz. *Elliptic curve cryptosystems*. Mathematics of Computation, 48, 1987.

[7] A. J. Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1993.

[8] V. Miller. *Use of elliptic curves in criptography*. CRYPTO'85, 1985.

[9] O. Morelló and S. Serramona. *Determinació del subgrup de 5-Sylow d'una corba el·líptica i generació de volcans de 5-isogènies*. Treball de Fi de Carrera, Universitat de Lleida, Setembre 2006.

[10] R. Moreno. *Subgrupos de Sylow de las curvas elípticas definidas sobre cuerpos finitos*. PhD thesis, Universitat Politècnica de Catalunya, 2005.

[11] D. Sardonil. *Curvas elípticas de cardinal par sobre cuerpos finitos y volcanes de 2-isogenias*. PhD thesis, Universidad de Valladolid, 2004.

[12] J. Vélu. *Isogénies entre courbes elliptiques*. Comptes Rendues de l'Académie des Sciencies de Paris, Série A, vol. 273, Académie des Sciences de Paris, juillet 1971.